

Notice of Allowability

Application No.

09/469,726

Examiner

Beemnet W. Dada

Applicant(s)

WANG, XIN

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to RCE filed on 10/11/07.
2. ☒ The allowed claim(s) is/are 1-22.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Stephen Hertzler, Reg No. 58,247 on 11/20/07.

The application has been amended as follows:

In the claims:

1. (Currently Amended) A method for encrypting an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising the steps of:

generating a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document;

encrypting the original document with the session key to create an encrypted document;

generating a proxy key based on a public key corresponding to the selected recipient, wherein the proxy key may be published without compromising its security, and wherein the proxy key, when applied to a document encrypted for a recipient, is used to transform the document ~~is operable to be used to transform a document encrypted for a recipient~~ into a document encrypted for another recipient without decrypting the message in the process; and

applying the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein the transformation may occur in a trusted environment without compromising its security, wherein the transformation may occur in an untrusted environment without compromising its security, and wherein the encrypted document remains in an encrypted state while being transformed into the transformed document and is not decrypted to the original document and re-encrypted at any point during the transformation.

13. (Currently Amended) A system operable to encrypt an original document for distribution to a selected recipient chosen from a plurality of possible recipients, comprising:

a session key generation system that generates a session key based on a random number privately maintained only by the owner, including an encryptor, of the original document;

an encryption system that encrypts the original document with the session key to create an encrypted document;

a proxy key generation system that generates a proxy key based on a public key corresponding to the selected recipient, wherein the proxy key may be published without compromising its security, and wherein the proxy key, when applied to a document encrypted for a recipient, is used to transform the document ~~is operable to be used to transform a document encrypted for a recipient into a document encrypted for another recipient without decrypting the message in the process;~~ and

a transformation system that applies the proxy key to the encrypted document to transform the encrypted document into a transformed document, wherein

the transformation may occur in a trusted environment without compromising its security,
wherein the transformation may occur in an untrusted environment without
compromising its security, and wherein the encrypted document remains in an encrypted
state while being transformed into the transformed document and is not decrypted to the
original document and re-encrypted at any point during the transformation.

Conclusion

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Beemnet W. Dada whose telephone number is (571)
272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30
pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for
the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the
Patent Application Information Retrieval (PAIR) system. Status information for published
applications may be obtained from either Private PAIR or Public PAIR. Status
information for unpublished applications is available through Private PAIR only. For
more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you
have questions on access to the Private PAIR system, contact the Electronic Business
Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO
Customer Service Representative or access to the automated information system, call
800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number:

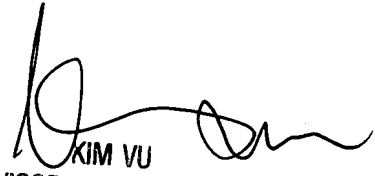
09/469,726

Art Unit: 2135

Page 5

Beemnet W Dada

November 20, 2007



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 210